Fool Proof Examination System through Color Visual Cryptography

Prof. Abhay R. Gaidhani[1], Pranjal Sansare[2], Sayali Wani[3], Mansi Singh[4], Gayatri waghchaure[5]
Department Of Computer Engineering, Sandip Institute Of Technology And Research Center, Nashik

Abstract: This paper proposes a new system of foolproof examination by tamperproof e-question paper preparation and secure transmission using secret sharing scheme. The application is perfectly secure because the proposed method automatically embeds the corresponding institute seal in the form of the key. As a result, it is easy to trace out the source culprit for the leakage of question papers. This scheme has reduced reconstruction time because the reconstruction process involves only Exclusive-OR (XOR) operation apart from authentication. The proposed method recovers the original secret image without any loss. The existing visual cryptographic scheme recovers half-toned secret image with average Peak Signal-to-Noise Ratio (PSNR) value 24dB. Further, it shall be stated that the proposed method with authentication recovers the image with 64.7dB PSNR value, which is greater than that of the existing method. In addition, this method does not suffer from pixel Expansion.

Keywords: Visual cryptography, secret sharing scheme, examination system, information security, authentication.

1. Introduction:

To achieve secure transmission of data, usually the data is concealed using symmetric or asymmetric key cryptography, which involves high computation and cost effective in encryption and decryption process. This project proposes a security system for tamperproof e-question paper sharing scheme using simple arithmetic operations. The secret sharing scheme has two categories–visual cryptography scheme and polynomial based secret sharing scheme.The main aim of this project is to overcome this drawback by employing secret sharing scheme for this application. The main concept of the original Visual Secret Sharing (VSS) scheme is to encrypt a secret image into number of meaningless share images. It cannot leak any information of the shared secret by combination of the share images except for all of the shares.

2. Literature Survey:

K. Shankar and P. Eswaran, RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique. K,Shankar ,P.Eswaran , A new k out of n secret image sharing scheme in visual cryptography, Intelligent Systems and Control (ISCO). Extension of their previous method . This time it is (k,n) scheme which was earlier (2,2).

Kulvinder Kaur,Vineeta Khemchandani. Securing Visual Cryptographic Shares using Public- Key Encryption , Advance Computing Conference Color image divided into 2 shares based on original technique and then encryption using RSA

Singh, V. K., Singh, P. K., & Rai, K. N. (2018). Image Encryption Algorithm based on Circular Shift in Pixel Bit Value by Group Modulo Operation for Medical Images. Image Encryption Algorithm based on Circular Shift in Pixel Bit Value by Group Modulo Operation.

K.Shankar , P. Eswaran , Sharing a Secret Image with Encapsulated Shares in Visual Cryptography. Sharing a Secret Image with Encapsulated Shares in Visual Cryptography.

Zhou, Z., Yang, C.-N., Cao, Y., & Sun, X. (2018). Secret Image Sharing Based on Encrypted Pixels.

Kashyap, P., & Renuka, A. (2019). Visual Cryptography for colour images using multilevel thresholding.

Li, P., Ma, J., Yin, L., & Ma, Q. (2020). A Construction Method of (2, 3) Visual Cryptography Scheme.

3. Project scope:

The main aim of this project is to overcome this drawback by employing secret sharing scheme for this application. The main concept of the original Visual Secret Sharing (VSS) scheme is to encrypt a secret image into number of meaningless share images. It cannot leak any information of the shared secret by combination of the share images except for all of the shares. The accuracy of the K-N share algorithm should be high and classification should be unambiguous.

4. System Working:

In k out of n visual cryptography scheme is a type of cryptographic technique where a digital image is divided into n number of shares by cryptographic computation. In the decryption process only k or more than k number of shares can reveal the original information [Here can form the original image]. Less than k number of shares can not reveal the original information. In this paper we have proposed an algorithm to divide a digital color image into n number of shares where minimum k numbers of shares are sufficient to reconstruct the image. If k numbers of shares are taken then the remaining shares are (n−k). In an image if certain position of a pixel is 1, then in (n−k)+1 number of shares in that position of that pixel there will be 1. In the remaining shares in that position of the pixel there will be 0. A random number generator is used to identify those number of shares. The Question Paper is encrypted into two shares so that the original image is visible only when the two shares are overlaid using Exclusive-OR (XOR) operation. The input question paper, generated shares, signatures of the examiner and the recovered question paper. The shares have the institution logo as an embedded watermark. As these shares contain the seal or logo of the institution or examination center, it is easy to identify the culprits leaking the question paper.

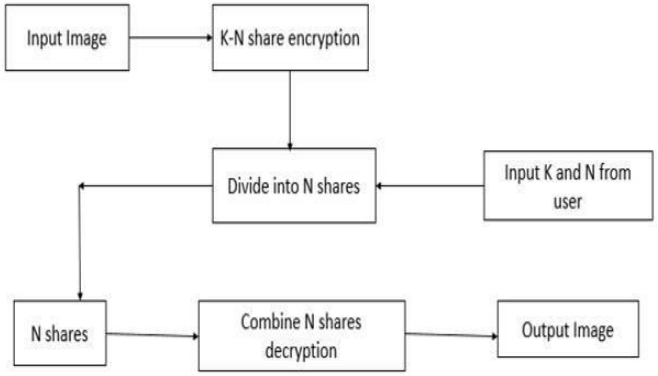
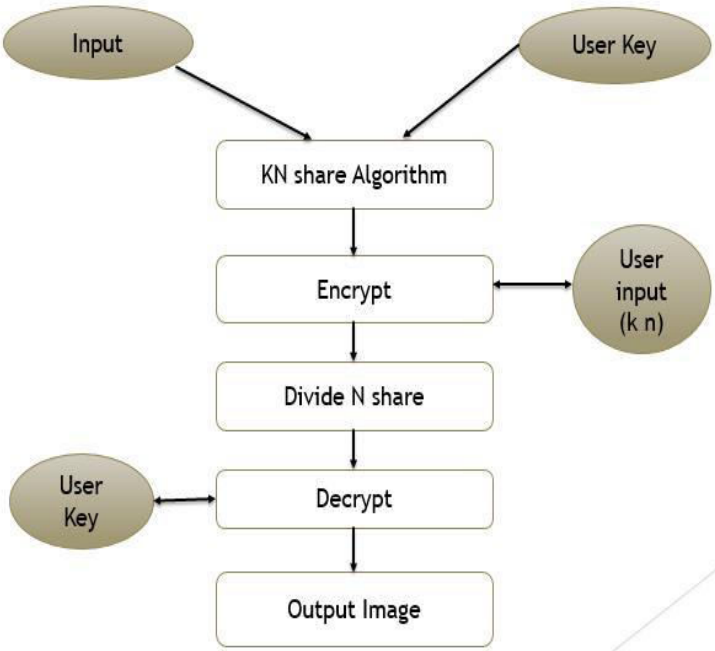


Figure- a) System Working

5. Algorithm:



Input: 1. 2 shares of size m*n
2 .key image k2 of any size

Step 1:

Apply decryption Algorithm to regenerate the question paper. Step 2:

Apply block based Encryption algorithm to produce shares using key k2.

Step 3:

Embed Signature of External Examiner in share 1.

Step 4:

Embed Signature of Internal Examiner in share 2

Step 5:

Distribute the share1 to Internal Examiner and Share 2 to External Examiner.

6. Conclusion:

This project suggests the automation of examination system by securing question paper using secret sharing scheme. The alternative methods for authentication will further enhance visual quality of images. To the best of our knowledge, color secret sharing scheme without half toning is applied for secure transmission of Examination question papers.

7. References:

1) Singh, Vineet Kumar, Piyush Kumar Singh, and K. N. Rai. "Image Encryption Algorithm based on Circular Shift in Pixel Bit Value by Group Modulo Operation for Medical Images." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.
2) Maurya, R., Kannojiya, A. K., & Rajitha, B. (2020). *An Extended Visual Cryptography Technique for Medical Image Security. 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA).*
3) Munir, R., & Harlili. (2018). *Encryption by Using Visual Cryptography Based on Wang's Scheme. 2018 4th International Conference on Electrical, Electronics and System Engineering (ICEESE).*
4) Li, P., Ma, J., Yin, L., & Ma, Q. (2020). *A Construction Method of (2, 3) Visual Cryptography Scheme.*
5) B. Shrivas and S. Yadav "Visual Cryptography in the Video using Halftone Technique" International Journal of Computer Applications (0975 – 8887) vol. 117 no. 14 May 2015.
6) Zhou, Z., Yang, C.-N., Cao, Y., & Sun, X. (2018). *Secret Image Sharing Based on Encrypted Pixels. IEEE Access, 6, 15021–15025.*
7) K.Shankar , P. Eswaran , Sharing a Secret Image with Encapsulated Shares in Visual Cryptography, Procedia Computer Science, Volume 70, 2015.
8) Singh, V. K., Singh, P. K., & Rai, K. N. (2018). *Image Encryption Algorithm based on Circular Shift in Pixel Bit Value by Group Modulo Operation for Medical Images.20184thInternational ConferenceonComputing Communication and Automation (ICCCA).*
9) K. Shankar and P. Eswaran, RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique, J CIRCUIT SYST COMP 25, 1650138 (2016).